

# Backdoors in Crypto



# The Problem with Castles.



# Treason Doors.



# Nottingham Castle.

- Roger Mortimer, 1st Earl of March ruled from Nottingham Castle.



NOTTINGHAM CASTLE IN THE SIXTEENTH CENTURY.

# Nottingham Castle.

- Roger Mortimer, 1st Earl of March ruled from Nottingham Castle.
- Nottingham Castle had a secret tunnel that bypassed all the defenses.



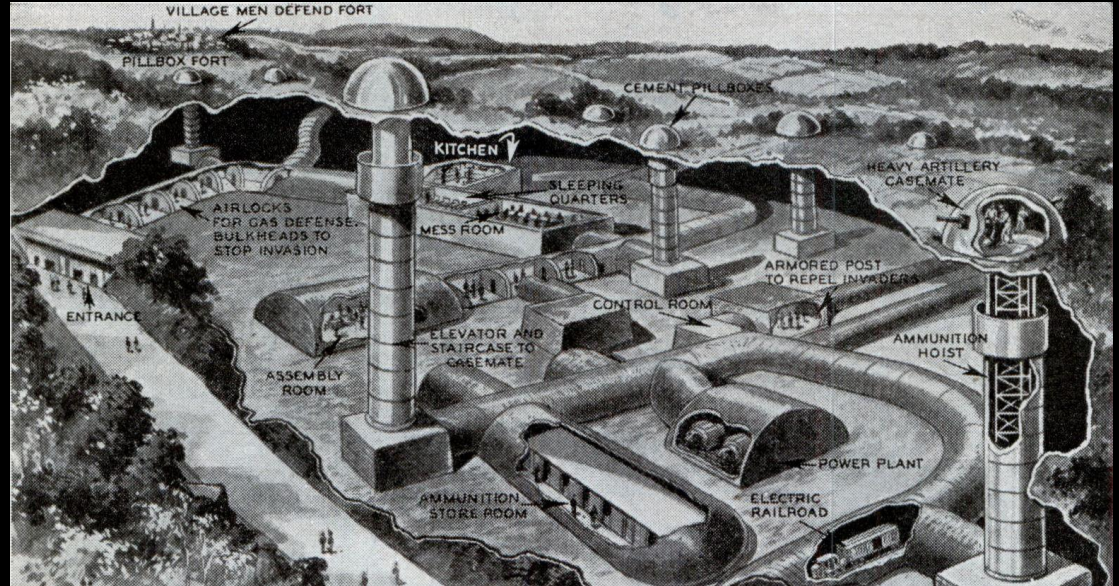
# Nottingham Castle.

- Roger Mortimer, 1st Earl of March ruled from Nottingham Castle.
- Nottingham Castle had a secret tunnel that bypassed all the defenses.
- 1330 AD - Secret passage isn't so secret.
  - Overseer of the castle betrays Mortimer.
  - Leads raid through secret tunnel.
  - kills Mortimer's guards, arrests Mortimer.
  - Mortimer is executed soon after.



# Maginot Line Fortifications.

- French WW2 fortifications.
- Claim: Designed so that if captured, they would be easier to recapture.



# What does this have to do with Crypto?

- Can you design a cipher that would keep you secure but you could break if other people used it?
- How?
- What properties should such a backdoor have?





# Backdoors Definition:

- Backdoors are built-in methods of bypassing the security of a system.



# Dual EC DRBG Backdoor: Overview

- Dual Elliptic Curve Deterministic Random Bit Generator.
- Backdoored by the NSA.
- Deployed in commercial systems.
- Exposed by Academic Cryptographers and Snowden.



# Dual EC DRBG Backdoor: How

- Dual Elliptic Curve Deterministic Random Bit Generator.
- Like Blum-Micali, but generates many bits at a time.

# Dual EC DRBG Backdoor: The players

- NSA - National Security Agency
  - Offensive/Defensive mission: Makes & breaks codes/ciphers,
  - Captures, listens to & analyzes communications.
- NIST - National Institute of Standards and Technology
  - Creates & evaluates national technology standards.
  - Trusted as a fair player nationally & internationally.
- RSA
  - Technology company, created to commercialize public key encryption.
  - Develops and sells encryption software/hardware to companies.

# Dual EC DRBG Backdoor: NIST

- NIST Crypto Contests:
  - NIST crypto standards.
  - Concern over NSA backdoor in DES.
  - Development of crypto contests.

# Dual EC DRBG Backdoor: NSA


- The NSA spends \$250m a year on a program which, among other goals, works with technology companies to "covertly influence" their product designs.
- Used by the NSA to "to leverage sensitive, co-operative relationships with specific industry partners" to insert vulnerabilities into security products. Operatives were warned that this information must be kept top secret "at a minimum"

**TOP SECRET STRAP1**

## Response to improving security

- For the past decade, NSA has lead an aggressive, multi-pronged effort to break widely used Internet encryption technologies
- Cryptanalytic capabilities are now coming on line
- Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable
- Major new processing systems, SIGDEV efforts and tasking must be put in place to capitalize on this opportunity

**PTD "We penetrate targets' defences."**

 This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221481 x30308 (non-sec) or email infoleg@gchq

© Crown Copyright. All rights reserved.

# Dual EC DRBG Backdoor: NSA

(U) Base resources in this project are used to:

- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.
- (TS//SI//REL TO USA, FVEY) Collect target network data and metadata via cooperative network carriers and/or increased control over core networks.
- (TS//SI//REL TO USA, FVEY) Leverage commercial capabilities to remotely deliver or receive information to and from target endpoints.
- (TS//SI//REL TO USA, FVEY) Exploit foreign trusted computing platforms and technologies.
- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.
- (TS//SI//REL TO USA, FVEY) Make specific and aggressive investments to facilitate the development of a robust exploitation capability against Next-Generation Wireless (NGW) communications.
- (U//FOUO) Maintain understanding of commercial business and technology trends.

# Dual EC DRBG Backdoor



- 2001 : CertiCOM licenses its EC technology to NSA.
- 2000 - 2004 ? : NSA adds Dual EC to ANSI X9.82 standard
- 2004 : NSA pays RSA 10m dollars to make Dual EC default in BSAFE library.
- 2005 : CertiCOM applies for public patent for EC backdoor method.
- 2005 : NIST publishes DRAFT SP-800-90A standard containing Dual EC.
- 2006 : Cryptographers discover backdoor possible & Dual EC is a bad RNG.
- 2006 : Despite weaknesses NIST standardizes SP-800-90A with Dual EC.
- 2007 : Other Cryptographers rediscover that Dual EC is backdoored.
- 2013-09 : Snowden leak shows NSA backdoored Dual EC.
- 2013-09 : NIST & RSA “don’t use Dual EC”, RSA denies knowledge.
- 2013-12 : Reuters releases story on secret RSA / NSA deal.
- 2014-04 : NIST revokes Dual EC standard (6 months ago)



# Effects



- Loss of trust in:
  - NIST standardization process at home and abroad,
  - USG & NSA's involvement in cryptographic development,
  - US technology companies esp cryptography & computer security.
- Presidential review setup:
  - recommends that the USG "fully support and not undermine efforts to create encryption standards".
- NIST is being held to a much higher degree of scrutiny.



# Other backdoors

- Crypto AG
  - Swiss cipher company sold machines to NATO and other countries.
  - After Suez crisis US wanted to listen to other NATO countries.
  - 1957 US got the owner of the company to slip backdoors into the machines so US could listen to NATO among others.
  - “Different countries need different levels of security”.
  - Revealed in 1977, but many countries were not paying attention.
  - Likely continues to this day.



# Other backdoors

- DES
  - Original version of DES, called Lucifer, had 128-bit key.
  - Was vulnerable to differential cryptanalysis.
  - NSA requested that the DES be shrunk to 48-bits, IBM resisted and they compromised on 56-bits.
  - 1977 DES becomes federal NIST standard.
  - 1998 EFF breaks DES in 54 hours with Deep Crack.

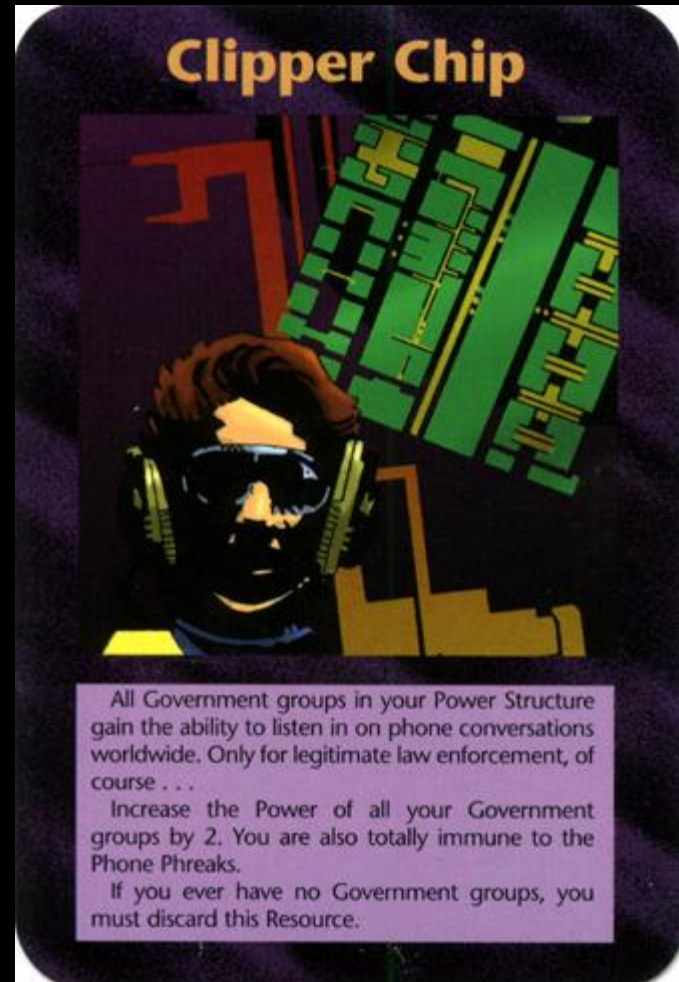


# Other backdoors

- Lotus Backdoor
  - Crypto export controls, encryption treated as a weapon.
  - Lotus forced to weaken crypto to export.
  - Key escrow.
  - “The idea was that they got permission to export 64 bit crypto if 24 of those bits were encrypted for the NSA’s public key.”
  - “I didn't know that our Notes keys were deposited (with the U.S.). It was interesting to learn this,” says Data Security Chief Jan Karlsson at the [Swedish] defense department.

# Other backdoors

- Clipper Chip.
  - Phone encryption standard.
  - Like lotus notes it is key escrow.
  - NSA was very public about the fact they could break it.
  - It was very poorly designed:
    - hackers broke it,
    - cryptographers broke it.
  - No one used it.



# Other backdoors

- "(TS//SI//REL TO USA, FVEY) Complete enable for [REDACTED] encryption chips used in Virtual Private Network and Web encryption devices"
- "(TS//SI//REL TO USA, FVEY) Exploit foreign trusted computing platforms and technologies."
- NSA installs implants when computers are shipped through the mail.
- On trusting trust.
- Are there more???

